A

Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	
First Inventor or Application Identifier	Anthony I. Provitola
Title	System of Secret Internet Web Sites, etc.
Express Mail Label No.	EJ356200814US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, DC 20231

1. ☒ * Fee Transmittal Form *(e.g., PTO/SB/17)*
(Submit an original and a duplicate for fee processing)
2. ☒ Specification [*Total Pages* 13]
(preferred arrangement set forth below)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings (*if filed*)
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
3. ☒ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 0]
4. Oath or Declaration [*Total Pages* 2]
   a. ☒ Newly executed (original or copy)
   b. □ Copy from a prior application (37 C.F.R. § 1.63(d))
   (for continuation/divisional with Box 16 completed)
      i. □ DELETION OF INVENTOR(S)
      Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

5. □ Microfiche Computer Program *(Appendix)*
6. Nucleotide and/or Amino Acid Sequence Submission (*if applicable, all necessary)*
   a. □ Computer Readable Copy
   b. □ Paper Copy (identical to computer copy)
   c. □ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. □ Assignment Papers (cover sheet & document(s))
8. □ 37 C.F.R.§3.73(b) Statement *(when there is an assignee)* □ Power of Attorney
9. □ English Translation Document *(if applicable)*
10. □ Information Disclosure Statement (IDS)/PTO-1449 □ Copies of IDS Citations
11. □ Preliminary Amendment
12. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. ☒ * Small Entity Statement(s) *(PTO/SB/09-12)* □ Statement filed in prior application, Status still proper and desired
14. □ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. □ Other: ....

16. If a **CONTINUING APPLICATION,** *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
□ Continuation □ Divisional □ Continuation-in-part (CIP) of prior application No: ______/______
Prior application information: Examiner ______ *Group / Art Unit:* ______
For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

□ *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bar code label here)* or ☒ *Correspondence address below*

Name	Anthony I. Provitola				
Address	Post Office Box 2855				
City	DeLand	*State*	Florida	*Zip Code*	32721-2855
Country	U.S.A.	*Telephone*	(904) 734-5502	*Fax*	(904) 736-3177

Name (Print/Type)	Anthony I. Provitola	*Registration No. (Attorney/Agent)*	
Signature		*Date*	Mar. 28, 2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

PTO/SB/06 (8-96)
Approved for use through 9/30/98. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD	Application or Docket Number

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY			OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE	FEE	OR	RATE	FEE
BASIC FEE (37 CFR 1.16(a))	▨	▨	▨	$ 345	OR	▨	$ ____
TOTAL CLAIMS (37 CFR 1.16(c))	minus 20 =	*	x $____=		OR	x $____ =	
INDEPENDENT CLAIMS (37 CFR 1.16(b))	minus 3 =	*	x ____=		OR	x ____ =	
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1 16(d))			+ ____ =		OR	+ ____ =	
			TOTAL	345	OR	TOTAL	

* If the difference in column 1 is less then zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY			OTHER THAN SMALL ENTITY	
AMENDMENT A	▨	CLAIMS REMAINING AFTER AMENDMENT	▨	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
	Total (37 CFR 1.16(c))	*	Minus	**	=	x $____=		OR	x $____ =	
	Independent (37 CFR 1.16(b))	*	Minus	***	=	x ____ =		OR	x _____=	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1 16(d))					+ _____ =		OR	+ ____ =	
						TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT B	▨	CLAIMS REMAINING AFTER AMENDMENT	▨	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
	Total (37 CFR 1 16(c))	*	Minus	**	=	x $____ =		OR	x $____ =	
	Independent (37 CFR 1 16(b))	*	Minus	***	=	x _____ =		OR	x _____ =	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1 16(d))					+ _____ =		OR	+ _____ =	
						TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT C	▨	CLAIMS REMAINING AFTER AMENDMENT	▨	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
	Total (37 CFR 1.16(c))	*	Minus	**	=	x $_____ =		OR	x $____ =	
	Independent (37 CFR 1 16(b))	*	Minus	***	=	x _____ =		OR	x _____ =	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1 16(d))					+ _____ =		OR	+ _____ =	
						TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) & 1.27(b))--INDEPENDENT INVENTOR

Docket Number (Optional)

Applicant, Patentee, or Identifier: Anthony I. Provitola

Application or Patent No.:

Filed or Issued: March 28, 2000

Title: SYSTEM OF SECRET INTERNET WEB SITES FOR SECURING USER ACCESS

As a below named inventor, I hereby state that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees to the Patent and Trademark Office described in:

☒ the specification filed herewith with title as listed above.
□ the application identified above.
□ the patent identified above.

I have not assigned, granted, conveyed, or licensed, and am under no obligation under contract or law to assign, grant, convey, or license, any rights in the invention to any person who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern, or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

☒ No such person, concern, or organization exists.
□ Each such person, concern, or organization is listed below.

Separate statements are required from each named person, concern, or organization having rights to the invention stating their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

Anthony I. Provitola		
NAME OF INVENTOR	NAME OF INVENTOR	NAME OF INVENTOR
Signature of inventor	Signature of inventor	Signature of inventor
March 28, 2000		
Date	Date	Date

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

SYSTEM OF SECRET INTERNET WEB SITES FOR SECURING USER ACCESS

The inventor is the applicant, Anthony I. Provitola, a citizen of the United States of America whose residence is DeLand, Florida, U.S.A.

CROSS-REFERENCE TO RELATED APPLICATIONS

Not Applicable

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not Applicable

REFERENCE TO MICROFICHE APPENDIX

Not Applicable

BACKGROUND OF THE INVENTION

Most, if not all, publicly accessible internet web sites are vulnerable to denial-of-service attacks. The precautions, safeguards and security systems that have been applied cannot adequately prevent the disruption of service without limiting access, and such remedies may be overcome by skilled and even unskilled attackers. In order to keep the internet open with minimum regulation it is necessary to have a system that sufficiently deters such attacks while maintaining significantly reduced vulnerability to such attacks. The current firewall and intrusion detection systems are largely powerless to halt distributed denial-of-service attacks. Even though scanners can alert administrators to computers used as attack conduits, known as "zombies", it is impossible to prevent the use of unsecured computers by attackers for that purpose. Among other similarly expedient precautions, the provision of alternative connections in the event of an attack, are ineffective if the existence and the universal resource locators (URLs) of the alternative connections are public information. The use of alternative connections for activities such as downloading is common. However, all of such associated alternative web sites become publicly known through the main web site publicly associated with the operator. However, it is not necessary to forego the advantage of such web site publicity if a system is implemented that will secure a user's access to a particular internet operation when the operator's main site is under attack, and thereby deter such attacks in the first place by rendering them futile and dangerous for the attacker in terms of the probability of detection and apprehension of the attacker. The present invention is a system of secret internet web sites, and a method for the use thereof, that provides the security desired while maintaining the openness, freedom, and anonymity of the internet.

BRIEF SUMMARY OF THE INVENTION

The present invention is a system of secret internet web sites which may be used to provide access to the internet web site operation of a given internet web site operator by persons intending to make normal use thereof when such access to such an operation has been compromised by cybervandalism, such as a denial-of-service attack, and a method for the use of such a system. If the number of such secret sites for access to a particular operator's internet operation are sufficient, it becomes extremely difficult for a denial-of-service attacker to disable such an operation through other computers connected to the internet which are used by attackers as distributed attack conduits. The system may be used in any given internet operation. A user of such an internet operation employs the system contacting the operator for that purpose. At the time of such contact the user is given the option of subscription by providing adequate information for the identification of the user. The user may elect not to provide such information, in which case the user may remain anonymous and continue to access the main site of such an operation, or any other site which is identified with the operator through the main site or otherwise. If the user does elect to provide such information for identification, the operator provides the user with a specific internet web site for access to the operator's internet operation, the URL of which is assigned specifically for access by the user and to be held as secretly as a password, a "secret site". Otherwise the user is free to contact and use the operator's main site anonymously as generally permitted and desired. Access to an operator's internet operation by a user may also be obtained by the use of the secret site system when the operator's main site is under denial-of-service attack by subscription through other means of contact, such as another internet operation that specializes in providing emergency contact or an automated telephone subscription system.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is a system of secret internet web sites which may be used to provide access to the internet web site operation of a given internet web site operator by persons intending to make normal use thereof when such access to such an operation has been compromised by cybervandalism, such as a denial-of-service attack, hereinafter referred to as an "attack", and a method for the use of such a system. The system which is the present invention will hereinafter be referred to as the "secret site system", and the term "system" as used hereafter shall refer to the secret site system unless otherwise indicated. As used in this disclosure a person intending to make normal use of an internet web site shall hereafter be referred to as a "user"; a person who attempts or engages in cybervandalism, such as a denial-of-service attack on an internet web site, shall hereafter be referred to as an "attacker"; and an entity which operates an internet web site publicly identified with that entity for the purpose of general and unrestricted initial access by the public shall hereafter be referred to as an "operator". An operator's internet web site which is publicly identified with a particular internet business or other activity of the operator shall hereafter be referred to as the "main site", which includes any other internet web site operated by the operator and publicly associated with such a main site; and the business or activity of the operator through a main site, including the authorship, programming and maintenance of the main site, shall be referred to as the operator's internet "operation".

For any given internet operation the system comprises a plurality of internet web sites, in addition to the main site of the internet operation, the URLs of which are not publicly associated with the operator, which shall hereinafter be referred to as "secret sites", that can provide access to the operator's internet operation conducted through the main site. The secrecy of a secret site derives from the fact that the URL for that site is maintained as a secret from all but those users who have been given the knowledge thereof by the operator, the URL then being held by the user as secretly as a password. Such knowledge is obtained by a user through assignment of a URL for a secret site by the operator to a user upon the user's request. The assignment of a secret site to a user is in response to the user providing means by which they can be sufficiently identified for purposes of the level of security against attack desired by the operator. Such assignment of a secret site may be coupled with other security measures such as passwords, encryption, and other software and hardware measures for detection and disruption of other forms of cybervadalism as well as the denial-of-service attack. If the number of such secret sites for access to a given operator's operation are sufficient, it becomes extremely difficult for an attacker to disable the service provided by the operator through "zombies", the internet connected computers used as distributed attack conduits.

Objects of the invention are to provide a system which secures access for users of an operator's internet web site operation when the operator's main site is under attack; thereby to effectively deter and thus prevent cybervandalism, such as denial-of-service attacks against publicly known web sites, by providing substantial opportunity for detection and apprehension of attackers.

The system operates with the cooperation of users who want to access the main site for the purpose of engaging the business or other internet activity of the operator. A user of such an internet operation employs the system by contact with the operator. The operator may be contacted through the operation's main site, by telephone, by mail, by e-mail, or by other means. At the time of such contact a user is given the option of subscription by providing adequate information for identification. If the user does elect to provide such information for identification, the operator provides the user with a specific internet web site with access to the operator's internet operation, the URL of which is secret for the user, a secret site. A secret site and its URL may be registered with the registration authority in any name lawfully useable by the operator, including fictitious names and controlled entities, with the object of avoiding association of the URL with the operator. The knowledge of the existence, identity and URL of a secret site are learned only through the process of subscription, such information not being otherwise available to the public. Subscription for the use of a secret site may be free, for a fee, or related to the regular fees otherwise charged for use of the main site by the operator. The user may elect not to provide such information for identification, in which case the user may remain anonymous and continue to rely upon access to the main site to engage the operator's operation, to the extent that the main site is available for access to users whose identity is not required. If such information is provided by a user, the extent of verification thereof is optional to the operator. Once the subscription process is complete the secret site may then be accessed by the user, if the user does not require anonymity for such access. In the event that the main site is under attack, the secret site may be accessed if the user decides that such access is neccessary at that time and the user is willing to forego anonymity. Otherwise the user is free to contact and use the main site anonymously as permitted and desired, using the secret site only in an emergency.

Subscription by a user for assignment of a secret site for a particular internet operation may also be effected while the main site for that operation is under attack. This may be accomplished by telephone or other contact with the operator. Again, such contact would be for the purpose of subscribing to obtain the URL of a secret site upon meeting the operator's requirements for identification of the user. A telephone subscription system based on telephone contact may be automated to provide a secret site URL following the touch tone key-in or voice/data recognition of such information for identification of the user as required by the operator, again with possible verification thereof. Such contact would require a source of information for the telephone number of the operator's telephone subscription system, such as a telephone directory, which may be available on the internet. The preferred embodiment of the method for use of the system with respect to subscription by a user during an attack employs another internet operation, one completely independent of the operation on the main site, that specializes in providing emergency subscription for users to secret site URLs as a service to various operators or users; again, by a process of identification of the user which meets the requirements for the particular internet operation to which secret site access is requested by the user. The system also includes the maintenance of a reserve of secret sites that would go on line in the event of an emergency created by an attack which was directed to some of the secret sites, such as those for which the URLs were learned by subscription or by dissemination by subscribers among potential attackers. Such emergency URLs could be communicated to users by e-mail, telephone, fax or other means by which a user would expect such a communication from the operator in such an emergency.

Inasmuch as operation of the main site is conducted through the use of a computer known as a web server, which is programmed to receive and transmit information over the internet, the web server for the main site may be programmed to implement the system which is the present invention. Such a program shall hereinafter be referred to as the "secret site program". The system may be made available through a web page which includes a secret site program for user subscription and operator assignment of a secret site URL. A secret site URL is one for which the operator has lawful use, either exclusive or non-exclusive, and which, in a preferred embodiment, should not be registered with any search engine database or made public in any way in which the secret site may be associated with the main site or the internet operation conducted thereon. The secret site program queries the user for the identification required by the operator, and proceeds to assign one of the secret site URLs to the user. In a preferred embodiment the user's identification information would be verified by the secret site program. Also in a preferred embodiment for non-emergency situations, that is, when the main site is not under attack, the secret site URL can be furnished to the user by mail, e-mail, fax or other means following verification of the user's identification information. In emergency as well as non-emergency situations the means for communication of the secret site URL to the user further identifies the user, or does not communicate the secret site URL at all.

A person who is a potential attacker may themselves also acquire knowledge of the URL of a secret site, but they must identify themselves to acquire such knowledge or acquire such knowledge through another user who is so identified. Because cybervandalism is usually conducted with anonymity, any enhancement of the traceability of the attacker denies advantage to the attacker, and thus deters attacks as well as giving advantage to persons attempting to identify and apprehend the attacker.

The secret site assigned to the user should, in a preferred embodiment, be one of many web sites of which the operator has lawful use as secret sites. The more secret sites that are available to the operator for assignment, and the more evenly the access of the users are distributed over the secret sites, the less likely cybervandalism, such as a denial-of -service attack, will disrupt the operator's overall internet operation, even if the operation conducted through the main site is compromised by the attack.

The system which is the present invention significantly increases the effort that would be required to mount an attack. Because an attack must affect many secret sites of an operation simultaneously, the likelihood of detection and apprehension of the attacker is significantly increased, thereby discouraging the attack in the first place. Moreover, the fact that any effect of an attack on a main site would be significantly blunted by the distribution of the main site's operation over many secret sites is itself a deterrent.

The system also increases the likelihood that the attack could be halted much sooner than would otherwise be possible. To enhance the deterrent effect of the system certain of the secret sites may be set up primarily for detection of attack situations, because the only circumstance in which such a secret site would be accessed would be for some form of attack, because no person would have a legitimate reason to access the site except through error.

Public knowledge of the use of the system in a particular internet operation is a further deterrent against attacks on the main and secret sites of that operation. The greater the recognition by a potential attacker of the futility of their effort, with the realization of the resources that would be required to mount the attack, would eliminate all but the most dedicated of attackers. However, because the most dedicated attackers are the more likely to be skilled, such attackers would also recognize the greater likelihood of detection and apprehension. Moreover it will be recognized by skilled attackers that the openness of the fact of the use of the system does not compromise the strategies and tactics that may be employed in using the system for detection and apprehension of attackers. Such strategies or tactics need not be made public in relation to maintaining the deterrent effect of the system.

The preferred embodiment of the system comprises a plurality of computers connected to the internet, some of which are programmed to operate as web servers, and some of which may host one or more web sites, including main sites and secret sites. The preferred embodiment also includes client computers and web servers operating according to programs which monitor each of the web servers hosting web sites associated with the operator's internet operation, including the secret sites. With the use of this embodiment of the system an attack may be detected as it occurs, partly by denial of service to some of such monitors, and partly by analysis of the internet activity by the programs of the monitoring computers and the programs of the web servers hosting the main and secret sites. The system thus increases the likelihood that the attack could be halted much sooner than would otherwise be possible. To further enhance the deterrent effect of the system certain of the secret sites may be set up primarily as decoys or for detection of attack situations, because the only circumstance in which such a secret site would be accessed would be for some form of attack, because no person would have a legitimate reason to access the site except through error.

The web servers for the main and secret sites and the monitoring computers may also be programmed to communicate by a network protected by firewall programming of those computers. Such a firewall would have to protect against the intrusion into and disruption of the monitoring and response activity of the system, as well as restricting access to the other tasks that the computers may perform.

CLAIMS

Claim 1. An internet operation including a system of secret internet web sites comprising:
a plurality of computers programmed to operate as web servers;
one or more of said web servers hosting internet web sites for said internet operation;
one or more of said internet web sites being main sites having URLs which are publicly associated with said internet operation accessible through said internet web sites;
one or more of said internet web sites being secret sites having URLs which are not publicly associated with said internet operation;
said secret sites being a part of said internet operation by which said internet operation may be accessed.

Claim 2. The internet operation of Claim 1 wherein the system of secret internet web sites is operated to secure said internet operation against cybervandalism.

Claim 3. The internet operation of Claim 1 wherein the system of secret internet web sites is operated to secure said internet operation against denial-of-service attacks.

Claim 4. The internet operation of Claim 1wherein one or more of said secret sites are assigned to one or more users of said internet operation.

Claim 5. The internet operation of Claim 1 wherein the URLs of secret sites are maintained as secret by entities authorized by the operator of the internet operation from all but those users who have been given the knowledge thereof by said operator.

Claim 6. The internet operation of Claim 1 wherein the URL of a secret site is acquired by a user through assignment to a user by an entity authorized by the operator.

Claim 7. The internet operation of Claim 1 wherein a secret site is one whose existence, identity and URL are learned by a user only through the process of subscription.

Claim 8. The internet operation of Claim 1 wherein the user is free to contact and use the main site anonymously as permitted and desired.

Claim 9. The internet operation of Claim 1 wherein a user may subscribe for a secret site URL while the main site is under attack.

Claim 10. The internet operation of Claim 1 wherein the telephone subscription system based on telephone contact is automated to provide a secret site URL.

Claim 11. The internet operation of Claim 1 wherein subscription by a user during an attack is through another internet operation, one completely independent of the operation on the main site.

Claim 12. The internet operation of Claim 1 wherein a reserve of secret sites is maintained that become available to the users of said internet operation in the event of an emergency created by an attack.

Claim 13. The internet operation of Claim 1 wherein the secret site program queries the user for the identification, verifies the information, and proceeds to assign one of the secret site URLs to the user.

Claim 14. A system of secret internet web sites, comprising:
a plurality of computers programmed to operate as web servers;
one or more of said web servers hosting internet web sites for an internet operation;
one or more of said internet web sites being secret sites having universal resource locators (URLs) which are not publicly associated with any internet operation;
which are operated to provide access to internet operations of other operators of internet web sites.

Claim 15. The system of secret internet web sites of Claim 14 wherein the system of secret internet web sites is operated to secure other internet operations against cybervandalism.

Claim 16. The system of secret internet web sites of Claim 14 wherein the system of secret internet web sites is operated to secure other internet operations against denial-of-service attacks.

Claim 17. The system of secret internet web sites of Claim 14 wherein the URLs of secret sites are maintained as secret by entities authorized by the operator of said system from all but those users who have been given the knowledge thereof by said operator.

Claim 18. The system of secret internet web sites of Claim 14 wherein the telephone subscription system based on telephone contact is automated to provide a secret site URL to subscribing users.

Claim 19. The system of secret internet web sites of Claim 14 wherein a reserve of secret sites is maintained that become available to the users of internet operation served by such a system in the event of an emergency created by an attack.

Claim 20. The system of secret internet web sites of Claim 14 wherein a secret site program queries a user for the identification information, verifies the information, and proceeds to assign one of the secret site URLs for access of the internet operation sought by the user.

ABSTRACT

A system of secret internet sites and an internet operation including such a system is used to permit access to the internet site operation of a particular internet site operator by persons intending to make normal use thereof when access to the site has been compromised by cybervandalism. This is accomplished by designation by a site operator of specific internet sites whose URLs are secret and have been assigned for the use of specific users who have previously identified themselves to the operator. A user's access to an operator's internet operation is thus secured when the operator's main site is under attack.

Please type a plus sign (+) inside this box → ⊞

PTO/SB/01 (12-97)
Approved for use through 9/30/00. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☒ Declaration Submitted with Initial Filing OR □ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	
First Named Inventor	Anthony I. Provitola
COMPLETE IF KNOWN	
Application Number	/
Filing Date	March 28, 2000
Group Art Unit	
Examiner Name	

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM OF SECRET INTERNET WEB SITES FOR SECURING USER ACCESS

(Title of the Invention)

the specification of which

☒ is attached hereto

OR

□ was filed on (MM/DD/YYYY) ________ as United States Application Number or PCT International Application Number ________ and was amended on (MM/DD/YYYY) ________ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
			□	□	□
			□	□	□
			□	□	□
			□	□	□

□ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)

□ Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box → [+]

PTO/SB/01 (12-97)
Approved for use through 9/30/00. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number *(if applicable)*

□ Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: □ Customer Number ______ → *Place Customer Number Bar Code Label here*
OR
□ Registered practitioner(s) name/registration number listed below

Name	Registration Number	Name	Registration Number

□ Additional registered practitioner(s) named on supplemental Registered Practitioner Information sheet PTO/SB/02C attached hereto.

Direct all correspondence to: □ Customer Number or Bar Code Label ______ *OR* ☒ Correspondence address below

Name	Anthony I. Provitola				
Address	Post Office Box 2855				
Address					
City	DeLand	State	Florida	ZIP	32721-2855
Country	U.S.A.	Telephone	(904) 734-5502	Fax	(904) 736-3177

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor: □ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])	Family Name or Surname
Anthony Italo	Provitola

Inventor's Signature						Date	3/28/00
Residence: City	DeLand	State	FL	Country	U.S.A.	Citizenship	U.S.A.
Post Office Address	Post Office Box 2855						
Post Office Address							
City	DeLand	State	Florida	ZIP	32721-2855	Country	U.S.A.

□ Additional inventors are being named on the ____supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto